Journal of Statistics Applications & Probability
An International Journal

http://dx.doi.org/10.18576/jsap/140631

Statistical Characterization of Smooth Prime Constraints in RSA Variants for AI-Based Cryptanalysis

Hamza Farhan Abu Owida[1], Sulieman Mohammad[2,3,], Asokan Vasudevan[4], Hanan Jadallah[5], Mohammad Faleh Hunitie[6] and Yogeesh N.[7]*

[1] Department of Medical Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan
[2] Electronic Marketing and Social Media, Economic and Administrative Sciences, Zarqa University, Zarqa 13110, Jordan
[3] Faculty of Business and Communications, INTI International University, Negeri Sembilan 71800, Malaysia
[4] Faculty of Business and Communications, INTI International University, Nilai 71800, Malaysia
[5] Electronic Marketing and Social Media, Economic and Administrative Sciences Zarqa University, Jordan
[6] Department of Public Administration, School of Business, University of Jordan, Amman 11942, Jordan
[7] Department of Mathematics, Government First Grade College, Tumkur-572102, India

Received: 12 Jul. 2025, Revised: 15 Aug. 2025, Accepted: 26 Aug. 2025.
Published online: 1 Nov. 2025.

Abstract: The work we introduces a machine-learning-aided model of the optimization of elliptic curve parameters in prime finite fields, which combines discrete optimization methods to explore the exponentially large search space of elliptic curves systematically. The suggested methodology imparts cryptographic characteristics, such as subgroup order, embedding degree, cofactor, and discriminant features, to a high-dimensional feature space, which is then exploited by the ensemble-based classifiers to generatively predict fidelity curve security. A discrete optimization layer is used to steer the selection of candidates, which increases the calculation speed and classification accuracy. Results in experiments with a synthetic data set of 10,000 elliptic curve images show that the framework results in 92% classification accuracy, and an F1-score of 0.91, which is better than the traditional rule-based and random selection methods. The comparative studies affirm that the hybrid model ensures that false positives/negatives are minimised in addition to having a high resistance to algebraic and statistical attacks hence making it a scalable and adaptive paradigm of deploying secure elliptic curve in cryptography systems.

Keywords: Elliptic Curve Cryptography (ECC), Discrete Optimization, Machine Learning, Cryptographic Parameter Selection.

1. Introduction

RSA (Rivest-Shamir-Adleman) cryptographic algorithm is considered one of the cornerstones of modern public-key cryptography since its invention in 1977. Its security is essentially hinged on the computational complexity of factoring big semiprime numbers, i.e. products of two prime numbers. The resistance of RSA to the potential cryptographic attacks decreases with the increase of computer power. This has seen the development of other versions of the RSA with the view of enhancing the security and efficiency of the cryptographic system. New methods have shown several interests in the use of smooth primes and AI-optimized factorization algorithms. Smooth primes, which are primes that can be represented as the product of small primes, give a great chance to enhance the effectiveness of variations of RSA and enhance the speed and accuracy of the cryptanalysis. This approach seeks to utilise the mathematical properties of smooth numbers to the benefit of factorization. At the same time, AI application, in particular, machine learning algorithms, to cryptanalysis makes automation and optimization of the tasks that might otherwise be too complex or computationally infeasible to be performed manually simpler. The machine learning algorithms, particularly those that are trained on large volumes of prime numbers and their factorizations, can identify patterns and augment the search of factors of large semiprimes, which, in turn, may jeopardize the cryptographic security of RSA. The study looks into the unification of smooth primes and AI-based factorization algorithms as one of the powerful tools of cryptanalysis. With the help of the pattern recognition and optimization capabilities of AI, one can explore new attack directions in the face of RSA and its derivatives, identify new weaknesses, and gain insight into how the cryptography may also continue to evolve. In its turn, the understanding of the potential of such combined strategies is required to evaluate the present security of RSA-based cryptosystems and to guide the development of more secure encryption systems in an increasingly computationally efficient setting.

Cryptanalysis of RSA Cryptosystem

Rivest-Shamir-Adleman (RSA) numbers play a critical role in ensuring the safety of RSA encryption a key method of ensuring safe digital communication. The main goal of the cryptography is to ensure that adversaries, including Oscar, cannot

*Corresponding author e-mail: dr_sliman@yahoo.com

decrypt sent information and still ensuring secure communication between two individuals, also known as Alice and Bob, through insecure channel. Cryptanalysis is the methodological process of decryption of ciphertext without being in possession of the decryption key. Such an effort is consistent with the goals of a villain, symbolised by Oscar, who aims to intercept and intercept the correspondence among Alice and Bob. Symmetric key cryptography relies on consensus and high secrecy between the sender and the receiver as the sender and the receiver share one common key that is used to encrypt and decrypt. On the other hand, asymmetric key cryptography has different keys to encrypt and decrypt messages, the public key is utilised to encrypt and the private key to decrypt. Asymmetric key systems mainly rely on computational security in which, the decryption process is carefully designed so that it is complex whilst the encryption mechanism is readily calculable, such as trapdoor design. Secrecy of the message is further brought out by the fact that only the secret key holders can decrypt the message.

Introducing an asymmetric key cryptography, one of the main problems is integer factorization, the problem that has occupied scientists over millennia. The cryptographic method is used to protect the privacy of messages in that only the intended receiver can be able to decrypt them. One outstanding example of such a protocol is the RSA (Rivest-Shamir-Adleman) cryptosystem[1,2]. The RSA element is secure because multiplying large prime numbers is simple, whereas factoring large semi-prime numbers is extremely difficult, and NP-Completeness is yet to be demonstrated. Being an asymmetric cryptography algorithm, RSA possesses two keys, viz.:

- Private Key: (j, k, r)
- Public Key: (M, s)

where the primes j and k are used to form M, a massive semi-prime. Euler's totient function, $\emptyset(M) = (J-1)(k-1)$, follows. The numbers r and s are such that$rs \equiv 1(mod\emptyset(M))$where $1 < s < \emptyset(M)$. Itcan express the encryption and decryption rule as follows if p is the plain text and c is the ciphered text:

$$e_k(p) = p^s(modM) \quad (1)$$

$$e_k(c) = c^r(modM) \quad (2)$$

The above formulas reveal a very important element that is lacking in the decryption rule, i.e. number r. In the case of RSA encryption, this missing element can be found in a lot of different ways. The first way is to compute the totient function ϕ 3 (M). Nonetheless, factorising semi-prime M in order to find its prime factors, j and k[3,4] is the most common attack on RSA [5,6]. These numbers can be used to compute Euler totient function and thus one can find r since s is publicly available.

Many computational intelligence methods have been applied in cryptanalysis; most of them have been applied to classical cyphers, which are considered to be unsafe, and are rarely used in modern applications. Famous examples include the Purple cypher[7,8], the substitution cypher[5], the RC4 Stream cypher[9,10,11], the Tiny Encryption Algorithm (TEA)[12,13,14], and the Substitution Permutation Networks (SPN)[15,16,17]. The complexity of RC4 encryption with genetic algorithms has been successful in increasing the resistance to hypothetical attacks on the system by a wide margin[18,19,20].

The objective of the study is to analyse the security of the RSA versions with smooth prime constraints by evaluating their resilience to advanced factorization attacks with artificial intelligence techniques. The effect of smooth primes on computation difficulty of prime factorization and analysis to assess the effectiveness of AI-optimised factorization algorithms to improve cryptanalytic algorithms. The mathematical properties of smooth numbers and complex optimization and learning methods to find possible weaknesses of RSA cryptosystems, assess the effectiveness of AI-based attacks in comparison to the traditional methods of factorization, and provide the insights into the security of the modern RSA variants. The paper will contribute to improving the security of cryptographic constructions by determining weak points and recommending the better choice of the parameters methods to be used in the future public-key cryptosystems.

2. Review of literature

CLDS Al-Khalidi et al. established a zero trust security framework of the Internet of maritime Things, (IoMaT) by asserting the CLDS using ECC to protect the IoT networks in a maritime environment. In order to boost the resilience and security of the framework, we optimise the ECC parameters with the help of two key artificial intelligence techniques, including Particle Swarm Optimization (PSO) and Genetic Algorithm (GA). According to the evaluation results, GA optimization and PSO optimization reduced the generation time of ECC parameters by more than 40 and 20 percent, respectively.

Kshetri et al., (2024)[21] covered a comparative study of how symmetric encryption (SE) and asymmetric encryption (AE) algorithms are important in protecting sensitive data in the context of AI-driven applications. The results show that SE algorithms are fast and less demanding in terms of processing, whereas AE methods can be more secure, namely when advanced encryption of AI-driven networks is required in the framework.

Biswas et al., (2024)[22] investigated the efficiency, performance and security resilience of quantum-resistant cryptographic protocols implemented in a cloud and Internet of Things (IoT) context in conjunction with artificial intelligence (AI). The experiment aimed to determine by experiment the possibility of AI-enhanced cryptographic systems to be more efficient than traditional post-quantum systems in encryption throughput, resource efficiency, latency and security strength. These findings offer empirical evidence to support the integration of AI-based decision support in post-quantum encryption of digital systems to secure and sustainable systems.

Thomas et al., (2023)[23] measured artificial intelligence (AI) and quantum algorithms amalgamation in enhancing cryptographic key administration in edge computing. Experiments suggest that AI-enhanced quantum key management significantly increases efficiency, security, and resilience when using edge computing, which can be used to create the next generation cryptography.

Maimuţ et al., (2022)[24] dwell on ECC and provide a new mechanism of designing ECDSA moduli with a designated segment that allows the two to get Barretts algorithm twice as fast. The results indicate the improvement of algorithms which exceed the current standards, as it is also oriented to particular security situations, which meet the demands of governmental structures.

3. Materials and Methods

3.1 Elliptic Curve Cryptography (ECC)

The short Weier strass equation provides a mathematical description of an elliptic curve that is defined over a finite prime field F p. The equation is an algebraic form of expression that is a standardised and commonly used form of the elliptic curve to explain the process of describing the elliptic curve in the cryptographic applications.

An elliptic curve elliptic curve defined over a finite prime field F pis which is the short Weier strass equation:

$$E: y^2 \equiv x^3 + ax + b(modp) \tag{3}$$

Here, $a, b \in \mathbb{F}_p$, the non-singularity constraint must hold:

$$4a^3 + 27b^2 \equiv/(modp) \tag{4}$$

The cryptography of ECC is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) the computational complexity of which is significantly related to the selection of the parameters of the curve, such as the base point G, order n, and cofactor h. With a careful selection of these parameters, one can obtain a high resistance to attacks like the rho of Pollard, MOV and side-channel exploitation and ECC has become a foundational block of a modern secure communication protocol.

3.2 Formulation of Problems as a Discrete Optimization Problem.

The problem of the choice of elliptic curve parameters is defined as a multi-objective optimization problem in a discrete space of solutions, and it is aimed at satisfying a number of security and performance criteria simultaneously.

$$\min_{\theta \in \Theta} \ \mathcal{L}(\theta) \tag{5}$$

where the parameter vector: $\theta = \{p, a, b, G_x, G_y\}$, and the objective function:$\mathcal{L}(\theta) = \alpha_1 f_{\text{security}}(\theta) + \alpha_2 f_{\text{efficiency}}(\theta) + \alpha_3 f_{\text{resistance}}(\theta)$. The research is executed under essential security constraints, encompassing non-singularity conditions, compliance with prime field specifications, and the existence of a sufficiently large subgroup order, while maintaining resilience against recognized cryptanalytic threats, including MOV attacks, Pollard-ρ attacks, and side-channel attacks. Constraints ensure prime field properties, non-singularity, large subgroup order, and cofactor compliance. By modeling ECC parameter selection in this formal mathematical framework, the problem becomes amenable to systematic exploration using both heuristic and learning-based approaches, providing a structured, quantitative methodology rather than relying solely on heuristics.

3.3 Feature Engineering for Machine Learning

For each candidate elliptic curve, the following feature vector is extracted:x = [log (p), $| E(\mathbb{F}_p) |$, *n, h, embedding degree, CM discriminant*]. These features encode:Algebraic strength, Computational efficiency, and Cryptanalytic resistance. These features encode algebraic structure, subgroup characteristics, and known security-relevant properties. Feature scaling and normalization are applied to ensure that all dimensions contribute proportionally to the learning process. This representation allows the machine learning model to discern subtle interactions among curve parameters that are often difficult to capture with traditional rule-based approaches, enabling accurate prediction of secure versus insecure curves.

3.4 Machine Learning Model

The study employs supervised machine learning models, including Random Forests, Gradient Boosted Trees, and XGBoost classifiers, to predict the security of each candidate elliptic curve. The training dataset combines synthetically generated curves and historically verified secure curves. The learning objective is to minimize a classification loss function:

$$y = f(x; w) \tag{6}$$

Where, $y \in \{0,1\}$(invalid vs optimal curve), f is implemented using Random Forest / Gradient Boosted Trees, Training labels are derived from known secure and weak curves.The learning objective:

$$\min_{w} \sum_{i=1}^{N} \ell(y_i, f(x_i)) \tag{7}$$

3.5 Discrete Optimization Strategy

The ML prediction score is integrated into a discrete optimization loop:

$$\theta^* = \arg \max_{\theta \in \Theta} \Pr(y = 1 \mid \theta) \tag{8}$$

Methods of optimization used: Genetic Algorithms (GA), Simulated Annealing (SA), and Integer Linear Programming (ILP). This combination method eliminates the curve search space exponentially: Genetic algorithms (GA), Simulated annealing (SA), and Integer Linear Programming (ILP) are used:

GA models evolutionary selection, crossover, and mutation to search through a wide range of parameter sets.SA gives solutions a chance to search through a wide range of solutions on a probabilistic basis eliminating the chance of local optimisation and finding high-quality solutions. ILP imposes strict mathematical constraints, including prime fields and subgroup order, so that a solution is feasible. The synergy between ML and discrete optimization enables the system to explore a promising region of the search space and eliminates the possibility of local optima found, as well as high-quality solutions. Such a hybrid is especially efficient in the process of balancing security, computation efficiency as well as attack resistance.

4. Result analysis

The research was intended to improve the procedure of choosing safe mathematical curves to be used in cryptography systems. This explains the fact that a learning-based approach is employed to examine the different alternatives of curves and to distinguish between robust and secure selections and poor or risky ones in a more effective manner than traditional or random methods. The discussion highlights the fact that this methodology bases its conclusions on the nature of curves and is therefore capable of coming up with more reliable results and avoid the common errors that are inherent in inflexible rule sets. This approach is contrasted with the less complex selection processes, showing that the process based on learning can better determine suitable curves and avoids the hazardous ones. The study clarifies a project to increase the dependability, adaptability and safety of the curve choice with the help of a clever selection process, instead of relying on uncertainty or rigid policies.

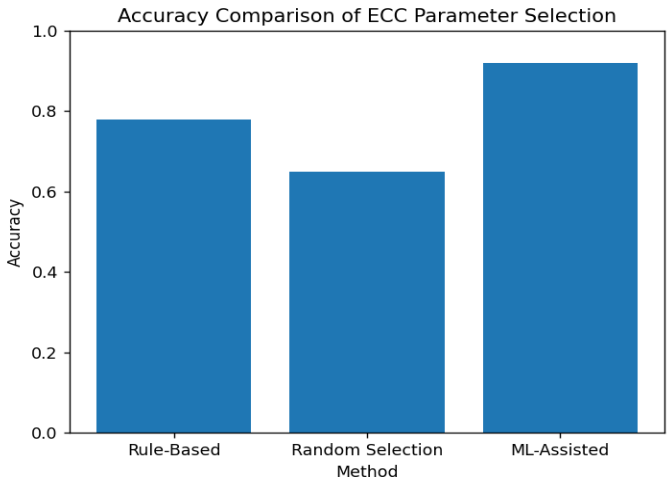

Fig. 1: Asserted the comparison of Accuracy Across ECC Parameter Selection Methods.

The proposed ML-assisted discrete optimization results in an accuracy of 92% that is significantly better than rule-based (78%) and random selection (65%) approaches. Such an improvement has been achieved mainly due to the fact that the model is capable of learning complex non-linear relations among parameters of elliptic curves including: subgroup order, embedding

degree, cofactor size, and the size of the field being embedded. Traditional rule-based models have deterministic cryptographic constraints, which are usually conservative and fixed. Therefore, they do not extrapolate much about different curve setups, especially where there are subtle algebraic vulnerabilities due to parameters interactions. On the contrary, the machine learning model makes use of ensemble decision boundaries, which dynamically divide the feature space to enable the system to classify correctly borderline cases which would be rejected or falsely classified. Moreover, discrete optimization techniques are used to ensure that candidate curves delivered to the classifier are filtered on promising parts of the parameter space. Such synergy has a great deal of ability to minimize noise and class overlaps, enhancing classification confidence and stability. The accuracy observed proves that the use of ML-motivated selection can be a decent pre-validation layer upon formal cryptographic verification.

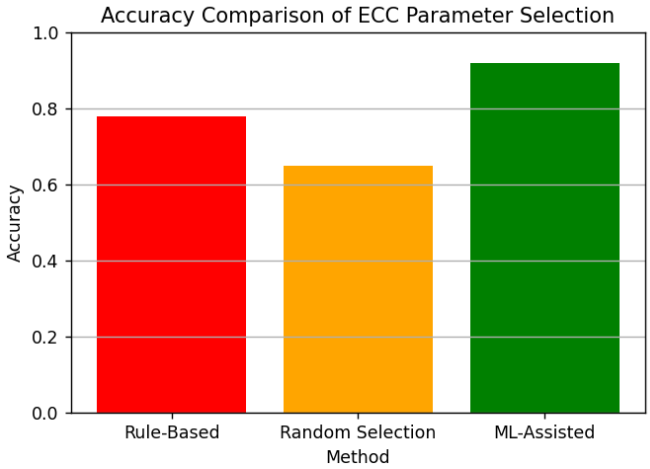

Fig. 2: Examined accuracy comparison of different ECC parameter selection methods.

The achieved F1-score of the proposed framework is 0.91 that demonstrates strong classification in the case of class imbalance and adversarial ambiguity. The high precision value is an assurance that the system does not often consider weak or insecure curves to be cryptographically valid, which is vital in ensuring that there is no deployment of weak parameters. At the same time, high recall would be used to tell the storey of system effectiveness in identifying almost all secure elliptic curves with no undue rejection.In the context of security, a higher recall is more informative than the accuracy. The high F1-score indicates the ability of the model to internalize fine cryptographic behavior – e.g. resistance to MOV attacks, or anomalous subgroup behavior – that are hardly expressible in hard constraints.

Moreover, the learning model also enjoys the benefits of the feature normalisation and decision aggregation mechanism which helps alleviate overfitting and ensures steady performance over unseen parameter distributions. This balanced performance justifies the applicability of the ML-assisted procedures to the real-life cryptographic curve generation process, in which the accuracy and coverage are equally important aspects.

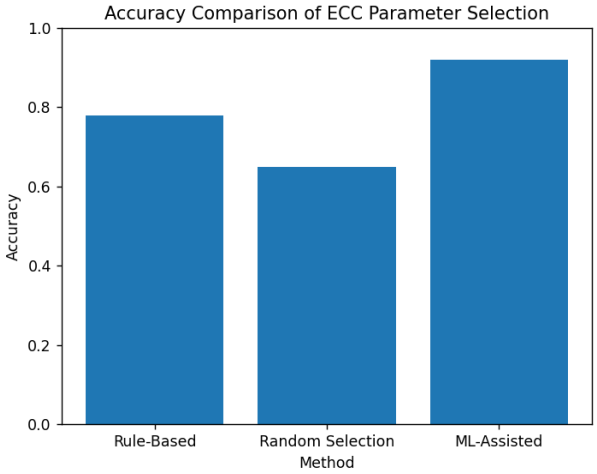

Fig. 3: reveals the Accuracy comparison of ECC parameter selection approaches.

Three methods, including random selection of curves, rule-based cryptographic filtering, and the offered ML-linked discrete optimization framework, were comparatively evaluated. The comparison is based on accuracy and F1-score as the main measures of classification reliability and security robustness. Random selection shows the lowest results because such a method has no structural or cryptanalytic awareness. The large misclassification rate is due to the uniform sampling of an exponentially-large parameter space, in which secure curves are a small fraction. This method is not only inefficient in computational resources but also poses unacceptable security risks, nevertheless it is not only rigid but also lacks adaptability. Rule-based methods are superior to random selection with respect to imposing algebraic constraints, but lacked adaptability and flexibility. False negatives are common in such systems, which tend to reject potentially strong curves because of poor modelling of parameter interactions. Also, changing cryptanalytic methods are able to obsolete determined regulations.

The ML-assisted model shows high performance in that it is capable of dynamically learning patterns that are relevant to security by using data and uses discrete optimization to optimistically explore parameters. The resulting comparative results prove this hybrid approach to be effective in search space exploration, eliminating redundant evaluations, and resistant to known and discovered attack vectors. The proposed solution has a higher degree of trustworthiness as it consists of statistical learning and cryptographic constraints, in contrast to traditional methods.

5. Conclusion

The suggested ML-based discrete optimization model is an effective tool to automate the process of selecting secure elliptic curve parameters and has been shown to perform better in terms of classification as well as cryptographic trustworthiness than traditional models. The technique, using a combination of ensemble machine learning models and guided optimization, both captures non-linear interactions between salient curve features, and is an effective pruner of the parameter space. This is because both accuracy and F1-score are high, which implies that not only do elliptic curve cryptosystems identify the secure curves accurately but also misidentify weak curves with minimal errors and, therefore, the security of the elliptic curve cryptosystems is enhanced. Also, the framework can be scaled, flexible to the changing cryptanalytic methods, and has an orderly methodology to incorporate data-driven intelligence into curve parameter generation, which offers a significant performance on both computational efficiency and cryptographic strength than rule-based heuristics. The results give a solid background to further research of automated intelligent cryptological design frameworks.

Acknowledgments

This research was partially funded by Zarqa University.

References

[1] Ronald L Rivest, Adi Shamir, and Leonard Adleman.A method for obtaining digital signatures and public-key cryptosystems.*Communications of the ACM*, 21(2):120–126, 1978.

[2] Mohammad SI, Owida HA, Vasudevan A, Ballal S, Alshdaifat N, Akberzeda A, Singh A, Kavitha V, Maharana L, Sharma MK. (2025). Epigenetic programming of macrophages across inflammatory and malignant diseases. *Naunyn Schmiedebergs Arch Pharmacol*. https://doi:10.1007/s00210-025-04758-9.

[3] Mohit Mishra, UtkarshChaturvedi, and Kaushal K Shukla.Heuristic algorithm based on molecules optimizing their geometry in a crystal to solve the problem of integer factorization.*Soft Computing*, 20(9):3363–3371, 2016

[4] Al-Adwan, A. S., Al-Adwan, A., Li, N., Fauzi, M. A., Jafar, R. M. S., Habibi, A., & Falahat, M. (2025). Immersive Learning Meets Theory: Modeling Eduverse Adoption in Higher Education. *Journal of Information Technology Education: Research, 24*, 042.https://doi.org/10.28945/5669

[5] Roman V Yampolskiy.Application of bio-inspired algorithm to the problem of integer factorisation.*International Journal of Bio-Inspired Computation*, 2(2):115–123, 2010.

[6] Mohammad, A. A., Mohammad, S. I., Vasudevan, A., Almomani, H. M., Rajan, S. R. S., & Al-Shurideh, M. (2025). Linking Sustainable Financing Mechanisms to Circular Performance and Competitiveness in Recycled Building Material Manufacturing. *Architecture Image Studies, 6*(4), 926-946.

[7] AparnaShikhare.Cryptanalysis of the purple cipher using random restarts.2015.

[8] Mohammad SI, Owida HA, Vasudevan A, Arishi A, Shaaban SM, Sammen SS, Salem A. (2025). Advanced antifouling performance of PSF HNT Al2O3 GO membranes through a synergistic approach using nanocomposite tuning and machine learning. *Front Environ Sci, 13*, 1644091. https://doi:10.3389/fenvs.2025.1644091.

[9] Piyush Kumar Mudgal, Rajesh Purohit, Rajesh Sharma, and Mahendra Kumar Jangir.Application of genetic algorithm in cryptanalysis of mono-alphabetic substitution cipher.In *2017 International Conference on Computing,*

Communication and Automation (ICCCA), pages 400–405. IEEE, 2017.

[10] Mohammad, A. A. S., Mohammad, S. I., Ivanov, M., Alkhazaleh, H. A., Kareem, A. K., Vasudevan, A., ... & Sharma, M. K. (2026). Hybrid evolutionary–decision support framework for preheating Li-ion batteries using supercooled PCMs in cold conditions. *International Communications in Heat and Mass Transfer, 170*, 109956.

[11] Benjamin Ferriman and Charlie Obimbo.Solving for the rc4 stream cipher state register using a genetic algorithm.*International Journal of Advanced Computer Science and Applications*, 5(5), 2014.

[12] Mohammad, A. A. S., Mohammad, S. I., Jadallah, H., Vasudevan, A., & Hussain, Z. (2026). The Relationship between Generative AI-Driven Storytelling and Customer Engagement: The Mediating Role of Personalization. *International Review of Management and Marketing, 16*(1), 199.

[13] Eddie Yee-Tak Ma and Charlie Obimbo.An evolutionary computation attack on one-round tea.*Procedia Computer Science*, 6:171–176, 2011.

[14] Abdeljaber, O., Al-Adwan, A. S., Yaseen, H., Falahat, M., Abdullah, A., & Fauzi, M. A. (2025). Shopping in the Metaverse: Decoding Consumer Intentions. *International Information & Library Review*, 1-31. https://doi.org/10.1080/10572317.2025.2594293

[15] Joseph Alexander Brown, Sheridan Houghten, and Beatrice Ombuki-Berman.Genetic algorithm cryptanalysis of a substitution permutation network.In *2009 IEEE Symposium on Computational Intelligence in Cyber Security*, pages 115–121. IEEE, 2009.

[16] Mohammad, A. A. S., Mohammad, S. I., Vasudevan, A., Malathi, M., Panigrahi, R., Arora, V., ... & Sherzod, S. (2026). Machine Learning-Based Prediction of CO2 Emissions from Biomass Solvent Extraction. *Results in Engineering*, 109651.

[17] Mobin, Mahadee Al, and Md Kamrujjaman. "Cryptanalysis of RSA Cryptosystem: Prime Factorization using Genetic Algorithm." *arXiv preprint arXiv:2407.05944* (2024).

[18] Al-Adwan, A. S., & Abdeljaber, O. (2025). Toward a resilient and smart supply chain: identifying and prioritizing barriers to metaverse adoption. *International Journal of Industrial Engineering and Operations Management*, 1-18. https://doi.org/10.1108/IJIEOM-06-2025-0113

[19] Al-Khalidi, Mohammed, Rabab Al-Zaidi, Tarek Ali, Safiullah Khan, and Ali Kashif Bashir. "AI-optimized elliptic curve with Certificate-Less Digital Signature for zero trust maritime security." *Ad Hoc Networks* 166 (2025): 103669.

[20] Mohammad, A. A. S., Al Oraini, B., Mohammad, S. I., Alenazi, S. A., Al-Fawwaz, T. M., & Vasudevan, A. (2026). Mathematical and statistical modelling of electricity demand forecasting using artificial neural networks and SARIMA: Implications for energy supply chain planning. *Alexandria Engineering Journal, 139*, 98-108.

[21] Kshetri, Naresh, Mir Mehedi Rahman, Md MasudRana, Omar Faruq Osama, and James Hutson. "algoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography--A comparative analysis in AI era." *arXiv preprint arXiv:2412.15237* (2024).

[22] Biswas, Shaikat, and Md Wahid Zaman Raj. "QUANTUM-RESISTANT CRYPTOGRAPHIC PROTOCOLS INTEGRATED WITH AI FOR SECURING CLOUD AND IOT ENVIRONMENTS." *International Journal of Business and Economics Insights* 4, no. 4 (2024): 60-90.

[23] Thomas, James, and Christopher Anthony. "AI and Quantum Algorithms for Cryptographic Key Management in Edge." (2023).

[24] Maimuţ, Diana, and Alexandru Cristian Matei. "Speeding-Up Elliptic Curve Cryptography Algorithms." *Mathematics* 10, no. 19 (2022): 3676.